Uwe Krause

(wip) Noch kein Titel

Fakultät Engineering and Computer Science
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Inhaltsverzeichnis

1 Motivation & Einleitung

1.1 Motivation: IT-(un)sicherheit allgemein

- (todo: aktuelle Quelle/Referenz)

1.2 Ziel: Programmierer verbessern

- Unsicherheit „greifbar“ machen
- um für die Einhaltung von „Secure coding Vorgaben“ / „best practices“ zu werben
  - (todo: Referenz??)
- (nicht Pentester ausbilden)

1.3 Didaktische Basis

- Active Learning [1]
- Blooms (revisited) Taxonomy [2]
- ICAP (Interactive - Constructive - Active - Passive) [3]

1.4 Vorgehen:

ctf als Elemente aus Pentester-„Ausbildung“ nutzen für Security Awareness bei Programmierern

- ctf as serious game
  - Designing a Serious Game for Cybersecurity Education [4]
  - Software Engineering for Games in Serious Contexts [5]

1.5 Diese Arbeit: Aufbau einer Beispiel-Challenge

In dieser Arbeit wird eine Beispiel-Challenge aufgebaut

1.5.1 Anforderungen an eine Challenge

- On the Requirements for Serious Games geared towards Software Developers in the Industry [6]

1.5.2 Evaluation

- Erfüllungsgrad der Anforderungen
- Vergleich mit anderen CTF
  - (Werte für andere CTF nicht selbst ermittelt: entommen aus Anforderungspaper)

2 Verwandte Arbeiten

Verschiedenste didaktische Konzepte bekräftigen, dass Lernende am erfolgreichsten lernen, wenn sie sich aktiv mit dem Lerngegenstand beschäftigen.

Beispielsweise ist eine der Grundprinzipien des „Active Learning“, die Lernenden „aktiv“ zu halten. Dieser Theorie zufolge ist das alleinige Lesen von Informationen oft nicht „aktiv“ genug. Solange Lernende sich nicht aktiv mit dem Lerngegenstand beschäftigen, werden sie dieser Theorie nach das Wissen nicht behalten. [1]

In Blooms Taxonomy gibt es verschiedene aufeinander aufbauende Ebenen. Nach den Ebenen „erinnern“ und „verstehen“ folgt die Ebene „anwenden“. Darauf wiederum folgen die Ebenen „analysieren“, „bewerten“ und „erschaffen“. [2]

Im ICAP-Ansatz (Interactive - Constructive - Active - Passive) werden vier Kategorien der kognitive Aktivitäten von Lernen definiert und unterschieden. Entlang dieser Kategorien erhöht sich das Lernen, wobei die Interaktion mit dem Lerngegenstand den besten Lernerfolg verspricht. [3]

2.1 Serious Games

Eine im IT-Sicherheitsbereich geeignete Form der Interaktion sind sogenannte „ernste Spiele“. Diese wurden entwickelt, um die Spieler über reale Themen wie Gesundheitsfürsorge, Sicherheit oder Umweltfragen aufzuklären, zu schulen oder zu informieren. [5]

Serious Gaming kann auch das Lernen komplexer und sehr technischen Themen erleichtern. Konzepte der IT-Sicherheit, können ebenfalls mit Techniken der „ernsten Spiele“

vermittelt werden. Es können fesselnde und kontrollierte Umgebungen geschaffen werden, in der sich Spieler realistischen Herausforderungen stellen können. [4]

Werden bei diesen ernsten Spielen IT-Security Techniken vermittelt, findet dies üblicherweise im Rahmen von „capture the flag“ statt. Es wurde von Trainings berichtet, in denen Teilnehmende großes Interesse am wettbewerbsorientierten Lernen zeigten [7] . Außerdem wurde gezeigt, dass mit capture the flag die Interaktion von Lernenden erhöht werden kann, was zu besser entwickelten Fähigkeiten führt [8] .

2.2 Anforderungen an ernste Spiele

Da (Software-) Projekte oft aufgrund fehlender oder ungenügender Anforderungsanalyse scheitern [9], wurden durch Kombination akademischer und industrieller Forschung 15 Anforderungen für Serious Games definiert, die sich an praktizierende Software-Entwickelnde richten [6] .

1. “Have a clearly defined learning goal objective”
2. “Adapted to background (job description) of participants developers”
3. “Well defined working mechanics (e.g. which tools to use or what to do)”
4. “Defined and progressive level of difficulty challenges”
5. “Elicit discussions of the solutions (e.g. is there a better/simpler way to solve?)”
6. “Provide possible solution after challenge solved”
7. “Adapted to the skill level of participants”
8. “Challenge includes hint that aid to arrive to the solution”
9. “Clear, standardized and simple solution (not based on obscure knowledge)”
10. “Planned duration of the exercise”
11. “Explains issues arriving from interplay of different technologies or components”
12. “Adapted to company internal secure coding guidelines and policies”
13. “Challenges are put from the defensive perspective”
14. “Solutions does not require specific knowledge of hacking tools”
15. “Challenges should raise awareness on possible consequences of malicious attack”

3 Aufbau der Challenge

3.1 Lernziel („learning goal objective“)

3.1.1 Übergeordnet

Broken Access Control

- Top 1 der aktuellen OWASP “Top 10 Web Application Security Risks”.

3.1.2 Konkret

Direkter Zugriff

- Direkte Anfrage nach Ressourcen, die aus der GUI nicht erreichbar wären CWE-425
- Auslesen von Meta-Daten, trotz fehlender Zugriffsberechtigungen CWE-200

Rechte-Ausweitung

- Rechte-Ausweitung (innerhalb der Anwendung)
  - ermöglicht durch fehlende Authorisationsprüfung CWE-862
- Rechte-Ausweitung (innerhalb der Plattform)
  - Initial-Modus, aktiviert, wenn keine Anwender registriert sind. Der erste registrierte Account wird dann mit Administrationsrechten ausgestattet. Der Zugriff zu diesem initial-Modus ist nicht eingeschränkt CWE-1188.
  - In Kombination mit einem unsicheren Anwender-Verwaltungs-Endpunkt, der es ohne Autorisation CWE-306 erlaubt Anwender zu löschen, kann ein Angreifer alle bestehenden Anwender, inklusive des bestehenden Administrations-Anwenders, löschen, um anschließend einen neuen Account anzulegen. Diesem wird nun von der Anwendung Administrationsrechte zugesprochen.

3.2 Storyline der Challenge

3.2.1 Aus Sicht des Programmierers

- Reddit ist erfolgreich
  - Kritik: zu offen, alles für alle lesbar, Leute mischen sich ein

Also: Schaffen einer privaten Austauschplattform „Glesn“.

- Hauptkonzept: „Spaces“
  - Themenbezogene Erfahrungs-Austausch-Kreise

- Zutritt nur auf Einladung (“invite only”)

Architektur

- Relationsmodell
  - User - Spaces - Artikel
- kurze Beschreibung Django
  - inklusive Besonderheit Django Admin

3.2.2 Aus Sicht des Betreibers

- Einfaches initiales Setup
  - Anmeldung: Erster Account hat Admin-Rechte
- Anlegen erster Spaces und Artikel
- Freigabe der Plattform für Anwender

3.3 Angedachter Lösungsweg der Challenge

Ausnutzen der platzierten Schwachstellen innerhalb der Anwendung

- Enumerieren der vorhandenen Artikel
- Auslesen der Meta-Daten (Spaces & Space-ID, Autoren und Autoren-ID)
- Rechte-Ausweitung innerhalb der Anwendung durch selbst-hinzufügen zu Administrator-Space, an der GUI vorbei, ermöglicht durch fehlende Autorisationsprüfung

Ausnutzen des initialen Setup-Modus

- Löschen aller Anwender
- Im Initialen Modus neuen Account
- mit diesem in die Administartions-Datenbank

3.3.1 Tipps und Hinweise für Lösungsweg

- Der erste Beitrag, der sichtbar ist, hat die ID 2
  - Hinweis darauf, dass es einen Eintrag mit der ID 1 geben müsste.
- Der erste Beitrag (ID 1) ist eine vom (simulierten Admin) angelegte Notiz an andere Admins
  - Der Admin drückt Freude darüber aus, wie einfach das initiale Setup dadurch war, dass das System einfach dem ersten User-Account Administrationsrechte gibt.

3.4 Realitätsbezug

2024 September: KIA

- News
  - Spiegel: Hacker konnten koreanische Autos per App orten, starten, hupen lassen
  - Heise: Kia: Lücken in Webportal erlaubten Forschern Fernzugriff auf Autos
  - Der Standard: Schwere Sicherheitslücken bei Kia ermöglichten Fernortung und Start von Millionen Autos
- Blog (Originalquelle)
  - Sam Curry: Hacking Kia: Remotely Controlling Cars With Just a License Plate

TODO: da werden sich schon noch Beispiele finden lassen

3.5 Beta-Test

Hamburger CTF-Team Cyclopropenylidene (C3H2)

- Feedback: ID für ersten sichtbaren Artikel sollte 2 sein, als Hinweis darauf, dass es einen weiteren Artikel (ID 1) gibt.
  - -> so umgesetzt
- Technisches Problem aufgedeckt: Ein Beta-Tester hat nicht nur einen Account angelegt und diesem (wie angedacht) einen Account Zugriff auf den versteckten Space gegeben, sondern mit Hilfe eines http replay Proxy die Sicherheitslücke so ausgenutzt, dass alle Accounts Zugriff auf den versteckten Space hatten. das hat dafür gesorgt, dass eine Beta-Testerin, die sich zuvor einen Account angelegt hat, aber die Sicherheitslücke noch nicht gefunden hat, plötzlich ohne eigenes zutun Zugriff auf den versteckten Space hatte.
  - -> Gelernt: Diese Challenge muss pro Person/Team als eigene Instanz bereitgestellt werden.

3.6 Durchführung Workshop

- Workshop Week an HAW September 2024
  - ca. 12 Teilnehmende
  - Studierende
    - Informatik

    - Bachelor
    - Master
  - Sonstige
- Evaluationsbögen
  - TODO: Ergebnis der Evaluationsbügen nutzbar?? (Jedenfalls nicht für direkten Vergleich!) (Eventuell noch ein Workshop notwendig??)

- IT-Security Konferenz „Nights of open Knowledge“ (NOOK)
  - 34 Teilnehmende
  - Allgemeines Feedback
    - Skala:
      - „auf jeden Fall“ / „eher ja“ / „eher nein“ / „auf keinen Fall“
    - Antworten
      - „War der Vortrag interessant?“
        - 12/12: „auf jeden Fall“
      - „Hat der Vortragende das Thema beherrscht?“
        - 12/12: „auf jeden Fall“
      - „Konnten Fragen beantwortet werden?“
        - 9/12 „auf jeden Fall“
        - 3/12 „eher ja“
      - „War das Material (Folien u.ä.) ansprechend?“
        - 10/12 „auf jeden Fall“
        - 2/12 „eher ja“
  - Es hat keine inhaltliche Evaluation stattgefunden

4 Ergebnis

4.1 Evaluation

TODO: Die entstandene Challenge so evaluieren wie in [6] beschrieben.

- semi-strukturierte Interviews ()
- Feedbackbogen (was hat gut funktioniert, was nicht)
- Fragebogen, Evaluationsfragen

Direkter Vergleich des Ergbenis der EIGENEN Challenge mit den Challenges aus dem Requirements-Paper [6]

Index	Requirement	Evaluation
1	Have a clearly defined learning goal objective	todo
2	Adapted to background (job description) of participants developers	todo
3	Well defined working mechanics (e.g. which tools to use or what to do)	todo
4	Defined and progressive level of difficulty challenges	todo
5	Elicit discussions of the solutions (e.g. is there a better/simpler way to solve?)	todo
6	Provide possible solution after challenge solved	todo
7	Adapted to the skill level of participants	todo
8	Challenge includes hint that aid to arrive to the solution	todo
9	Clear, standardized and simple solution (not based on obscure knowledge)	todo
10	Planned duration of the exercise	todo
11	Explains issues arriving from interplay of different technologies or components	todo
12	Adapted to company internal secure coding guidelines and policies	todo
13	Challenges are put from the defensive perspective	todo
14	Solutions does not require specific knowledge of hacking tools	todo
15	Challenges should raise awareness on possible consequences of malicious attack	todo
		?? %

Abbildung 1: Evaluationsergebnis

- Ergebnis (hoffentlich): meine Challenge erfüllt die Anforderungen besser

4.2 Diskussion

Die Evaluation zeigt, dass

- …?
- Zielgrupopenorientiertheit (zugeschnitten auf Jobtitle) weiterhin schwierig
- … ?

- Challenges are put from the defensive perspective
  - not fulfilled??
- ...?

5 Fazit

. . .

5.1 Ausblick

Durch einen „import“ anderer „Modelle“ aus dem Unterhaltungsbereich könnten „Empfehlungen für Verbesserungen und Erkenntnisse zur Gestaltung und Entwicklung effektiverer SG [Serious Games]“ übernommen werden [10]

Die durchgeführte Evaluation sowohl der bestehenden CTF-Events als auch der entwickelten Challenge ist ausbaufähig.

Ein konkretes Beispiel für die Übernahme von bestehenden Methoden aus der Unterhaltungsmedien-Entwicklung könnte ergänzend oder anstelle der durchgeführten Evaluation Evaluations-Methoden aus der allgemeinen Spiele-Entwicklung oder dem Übergeordneten Feld der „serious games“ auch auf die entwickelte/n Challenge/s adaptiert werden. Ansätze hierfür finden sich zum Beispiel in [User Experience Evaluation Methods for Games in Serious Contexts] [11] oder [Framework for evaluating Capture the Flag (CTF) security competitions] [12]

Wird das Feedback der Teilnehmenden ernst genommen und liefern die Evaluations-Methoden gute Einblicke, lassen sich die somit ermittelte Erfahrungen wieder als Anforderungen formulieren, um die bestehenden Anforderungen zu verfeinern oder zu ergänzen.

Bibliographie

[1] J. Eckstein, J. Bergin, und H. Sharp, „Patterns for active learning“, in *Proceedings of PLOP*, 2002.

[2] L. W. Anderson und D. R. Krathwohl, Hrsg., „A taxonomy for learning, teaching, and assessing: a revision of Bloom's taxonomy of educational objectives“. Longman, New York, 2001.

[3] M. T. H. Chi und R. Wylie, „The ICAP Framework: Linking Cognitive Engagement to Active Learning Outcomes“, *Educational Psychologist*, Bd. 49, Nr. 4, S. 219–243, Okt. 2014, doi: 10.1080/00461520.2014.965823.

[4] G. Costa und M. Ribaudo, „Designing a Serious Game for Cybersecurity Education“, *Software Engineering for Games in Serious Contexts*. Springer Nature Switzerland, Cham, S. 265–290, 2023. doi: 10.1007/978-3-031-33338-5_12.

[5] K. M. L. Cooper und A. Bucchiarone, Hrsg., „Software Engineering for Games in Serious Contexts“. Springer Nature Switzerland, Cham, 2023. doi: 10.1007/978-3-031-33338-5_12.

[6] T. Espinha Gasiba, K. Beckers, S. Suppan, und F. Rezabek, „On the Requirements for Serious Games Geared Towards Software Developers in the Industry“, in *2019 IEEE 27th International Requirements Engineering Conference (RE)*, Jeju Island, Korea (South): IEEE, Sep. 2019, S. 286–296. doi: 10.1109/RE.2019.00038.

[7] Computer Science Department, Texas Tech University, A. Siami Namin, Z. Aguirre-Muñoz, Texas Tech University, K. Jones, und Texas Tech University, „Teaching Cyber Security through Competition An Experience Report about a Participatory Training Workshop“, in *7th Annual International Conference on Computer Science Education: Innovation & Technology (CSEIT 2016)*, Global Science & Technology Forum (GSTF), Okt. 2016. doi: 10.5176/2251-2195_CSEIT16.39.

[8] K. Leune und S. J. Petrilli, „Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education“, in *Proceedings of the 18th Annual Conference on Information Technology Education*, Rochester New York USA: ACM, Sep. 2017, S. 47–52. doi: 10.1145/3125659.3125686.

[9] H. Ghanbari, J. Similä, und J. Markkula, „Utilizing online serious games to facilitate distributed requirements elicitation“, *Journal of Systems and Software*, Bd. 109, S. 32–49, Nov. 2015, doi: 10.1016/j.jss.2015.07.017.

[10] V. Wanick, J. Stallwood, und G. Xavier, „Future Directions in Games for Serious Contexts: A Conversation About Transferability“, *Software Engineering for Games in Serious Contexts*. Springer Nature Switzerland, Cham, S. 137–153, 2023. doi: 10.1007/978-3-031-33338-5_7.

[11] S. Kirginas, „User Experience Evaluation Methods for Games in Serious Contexts“, *Software Engineering for Games in Serious Contexts*. Springer Nature Switzerland, Cham, S. 19–42, 2023. doi: 10.1007/978-3-031-33338-5_2.

[12] R. Raman, S. Sunny, V. Pavithran, und K. Achuthan, „Framework for evaluating Capture the Flag (CTF) security competitions“, in *International Conference for Convergence for Technology-2014*, Pune, India: IEEE, Apr. 2014, S. 1–5. doi: 10.1109/I2CT.2014.7092098.